Homeland Security

Daily Open Source Infrastructure Report
02 July 2015

Top Stories

- Interstate 70 at Interstate 270 in Columbus, Ohio was closed indefinitely July 1 after a semi-truck hauling 10,000 gallons of ethanol-based chemical fuel overturned and caught on fire. – *Columbus Dispatch* (See item **4**)

- New York officials reported June 30 that 12 more Clinton Correctional Facility employees were put on administrative leave as part of an ongoing investigation into the escape of two murder convicts June 6. – *Associated Press* (See item **12**)

- Apple released iOS version 8.4 addressing 33 security vulnerabilities, including a fix for the Logjam flaw that allows a man-in-the-middle attacker to downgrade cryptographic security. – *Softpedia* (See item **15**)

- The FBI is investigating at least 11 physical attacks on high-capacity Internet cables in California's San Francisco Bay Area dating back to July 2014. – *USA Today* (See item **18**)

Energy Sector

1. *June 30, Associated Press* – (California) **Electrical vault blast leaves 17,000 without power in LA.** A June 30 explosion in an electrical vault in Los Angeles caused about 17,000 customers to lose power. The Los Angeles Department of Water and Power is investigating the cause of the blast and reports that power should be restored July 1.
Source: http://www.sacbee.com/news/state/california/article25951696.html

2. *June 30, Tallahassee Democrat* – (Florida) **30,000 in Tallahassee without power.** Talquin Electric Cooperative officials reported June 30 that about 20,000 customers were without power following heavy storms that swept through the area, and that service could take up to 24 hours to be restored.
Source: http://www.wtsp.com/story/news/2015/06/30/30000-in-tallahassee-without-power/29540891/

For another story, see item **4**

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

See item **11**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

3. *June 30, Reuters* – (National) **Goldman settles SEC charges over 2013 trading incident.** Goldman Sachs Group Inc., agreed to pay $7 million June 30 to resolve U.S.

Securities and Exchange Commission charges connected to the "market access" rule, and a 2013 programming error which flooded the stock options market with about 16,000 erroneous orders, causing 1.5 million options contracts to be executed and costing the company $38 million.
Source: http://www.reuters.com/article/2015/06/30/sec-goldmansachs-idUSL1N0ZG1JH20150630

[Return to top]

Transportation Systems Sector

4. *July 1, Columbus Dispatch* – (Ohio) **I-70 still closed after crash on West Side.** Interstate 70 at Interstate 270 in Columbus is closed indefinitely July 1 after a semi-truck hauling 10,000 gallons of ethanol-based chemical fuel overturned and caught on fire. The driver was taken to an area hospital and a team from the Ohio Environmental Protection Agency was on scene to respond to the chemical fumes.
Source: http://www.dispatch.com/content/stories/local/2015/07/01/fiery-crash-closes-i270-i70-on-west-side.html

5. *June 30, Bell Jar News* – (Colorado) **United Airlines flight diverted after man caught smoking in bath.** A United Airlines flight headed to Boston returned to Denver International Airport June 30 shortly after takeoff after a passenger refused to stop smoking onboard. The flight was cancelled due to crew rest regulations.
Source: http://www.belljarnews.com/united-airlines-flight-diverted-after-man-caught-smoking-in-bath/8512528/

[Return to top]

Food and Agriculture Sector

6. *July 1, Food Safety News* – (North Carolina) **232 sickened in outbreak linked to North Carolina restaurant.** The North Carolina Department of Health and Human Services reported June 30 that 232 people were sickened June 16 – June 21 due to salmonella contamination found in food products from the Tarheel Q restaurant in Lexington, North Carolina. An investigation is ongoing to determine further contaminations.
Source: http://www.foodsafetynews.com/2015/07/at-least-30-sickened-after-dining-at-north-carolina-restaurant/#.VZPP7flVhBc

[Return to top]

Water and Wastewater Systems Sector

See item **9**

[Return to top]

Healthcare and Public Health Sector

7. *June 30, Time Warner Cable News* – (Texas) **Austin Regional Clinic bans children of anti-vax parents.** Austin Regional Clinic in Texas began refusing treatment for unvaccinated children starting July 1, citing concerns over illnesses such as whooping cough, chicken pox, and measles which are easily transmitted in hospital waiting rooms.
Source: http://www.twcnews.com/tx/austin/news/2015/06/30/austin-regional-clinic-bans-children-of-anti-vax-parents.html

8. *June 30, Indianapolis Star* – (Indiana) **Community Health to pay $20 million in fraudulent billing settlement.** The U.S. Attorney's Office announced June 30 a $20 million settlement with Community Health Network, in central Indiana, after allegations that the health care network submitted fraudulent surgery bills to Medicare and Medicaid between 2006 and 2009.
Source: http://www.indystar.com/story/news/crime/2015/06/30/community-health-pay-million-fraudulent-billing-settlement/29511889/

[Return to top]

Government Facilities Sector

9. *June 30, Jersey Journal* – (New Jersey) **About 40 Jersey City Heights residents, school affected by water main break.** St. Nicholas School in Jersey City Heights was closed June 30 after a water main break on Ferry Street. Nearby residents have been notified of the break and crews are working to repair the water main.
Source:
http://www.nj.com/hudson/index.ssf/2015/06/40_jersey_city_heights_residents_school_affected_b.html

10. *June 30, Cincinnati Enquirer* – (Ohio) **Perfume bottle sparks scare, courthouse closure.** A perfume bottle shaped like a grenade was discovered during a security screening of a suitcase at Hamilton County Courthouse June 30, prompting officials to evacuate the building after a bomb-sniffing dog alerted deputies the bag was suspicious. The courthouse reopened July 1.
Source: http://www.cincinnati.com/story/news/2015/06/30/courthouse-evacuated-suspicious-package/29502849/

[Return to top]

Emergency Services Sector

11. *July 1, WHIO 7 Dayton* – (Ohio) **Fire crews remain on scene of industrial fire.** An industrial fire at Genesis Rescue Systems in Kettering, Ohio prompted fire crews to remain on site for several hours after the facility and its contents sustained extensive damage June 30. Total damages are unknown and no injuries were reported.
Source: http://www.whio.com/news/news/local/fire-reported-at-kettering-

business/nmpfj/

12. *June 30, Associated Press* – (New York) **NY prison chief, 11 others put on leave after escapes.** New York officials reported June 30 that 12 more employees at the Clinton Correctional Facility have been put on administrative leave as part of an ongoing investigation to find potential accomplices in the escape of two murder convicts June 6.
Source: http://www.policeone.com/investigations/articles/8633939-NY-prison-chief-11-others-put-on-leave-after-escapes

13. *June 30, WJW 8 Cleveland* – (Ohio) **Westlake police officer indicted for using excessive force on suspect.** The U.S. Attorney's Office reported June 30 that a former-Westlake police officer was indicted for 1 count of excessive force and 2 counts of obstruction from an April 2014 incident in which the officer caused bodily harm to a suspect and falsified documents.
Source: http://fox8.com/2015/06/30/westlake-police-office-indicted-for-using-excessive-force-on-suspect/

[Return to top]

Information Technology Sector

14. *July 1, Securityweek* – (International) **Attackers abuse RIPv1 Protocol for DDoS reflection: Akami.** Security researchers from Akami discovered that malicious actors have been leveraging routers running Routing Information Protocol version 1 (RIPv1) to reflect distributed denial-of-service (DDoS) attacks by creating malicious requests for routes and then spoofing the source Internet protocol (IP) address to match the one of the targeted system.
Source: http://www.securityweek.com/attackers-abuse-ripv1-protocol-ddos-reflection-akamai

15. *July 1, Softpedia* – (International) **iOS 8.4 fixes 33 security vulnerabilities.** Apple released iOS version 8.4 addressing 33 security vulnerabilities, including a fix for the Logjam flaw that allows a man-in-the-middle (MitM) attacker to downgrade cryptographic security, and other protection against potential arbitrary code execution.
Source: http://news.softpedia.com/news/ios-8-4-fixes-33-security-vulnerabilities-485771.shtml

16. *July 1, Softpedia* – (International) **Researchers expose attack on iOS that can break system apps.** Security researchers from FireEye reported two Apple iOS flaws, dubbed Manifest Masque and Extension Masque, in which an attacker could break or replace system apps and extensions on an affected device by taking advantage of apps created in Xcode outside of Apple's App Store. The vulnerabilities behind Manifest Masque attacks were partially addressed in the release of iOS 8.4.
Source: http://news.softpedia.com/news/researchers-expose-attack-on-ios-that-can-break-system-apps-485756.shtml

17. *June 30, Securityweek* – (International) **ESET analyzes complex espionage platform used by "Animal Farm" APT.** ESET released research on the Dino cyber-espionage platform used by the "Animal Farm" advanced persistent threat (APT) group revealing that Dino is capable of retrieving information, executing Microsoft Windows batch commands, searching for files, and transferring files back and forth between a command and control (C&C) server. Researchers have not determined the tool's initial infection vector.
Source: http://www.securityweek.com/eset-analyzes-complex-espionage-platform-used-animal-farm-apt

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

18. *July 1, USA Today* – (California) **FBI investigating 11 attacks on San Francisco-area Internet lines.** The FBI is investigating at least 11 physical attacks on high-capacity Internet cables in California's San Francisco Bay Area as far back as least July 2014, including a June 30 incident that disrupted Internet service for businesses and residential customers near the Sacramento area.
Source: http://www.usatoday.com/story/tech/2015/06/30/california-internet-outage/29521335/

19. *June 30, The Oregonian/OregonLive.com* – (Oregon; Washington) **Frontier suffers big cable TV outage.** Level 3 Communications officials reported that service was restored June 30 after Frontier Communications' cable TV service experienced an outage in Oregon and Washington due to severed communications fiber-optic cable earlier that day.
Source: http://www.oregonlive.com/silicon-forest/index.ssf/2015/06/frontier_suffers_big_cable_tv.html

For additional stories, see items **15** and **16**

Commercial Facilities Sector

20. *July 1, WCSC 5 Charleston* – (South Carolina) **Fire destroys Mt Zion AME church in Williamsburg County.** A 3-alarm fire at the South Carolina Mount Zion AME Church in Williamsburg County sustained extensive damage to its facility and injured 1 firefighter June 30. Fire crews contained the incident and the cause of the blaze is

unknown.
Source: http://www.walb.com/story/29447600/fire-destroys-mt-zion-ame-church-in-williamsburg-county

21. *July 1, WJLA 7 Denver* – (Colorado) **2-alarm fire damages apartment, business on Newton Street.** Westminster, Colorado fire officials reported July 1 that a mixed-use building housing commercial businesses and apartments sustained heavy damages after a 2-alarm fire destroyed 2 levels of the structure June 30. No injuries were reported and the cause of the fire is under investigation.
Source: http://www.thedenverchannel.com/news/front-range/westminster/2-alarm-fire-damages-apartment-business-on-newton-street

22. *July 1, WXIA 11 Atlanta* – (Georgia) **Video: 2 children jump from window to escape fire.** A June 30 fire at the Morgan's Landing Apartments in Sandy Springs, Georgia displaced 29 residents and 11 families as the fire burned through several apartment units. The cause of the fire is under investigation and no injuries were reported.
Source: http://www.11alive.com/story/news/local/sandy-springs/2015/06/30/sandy-springs-apartment-fire/29519425/

[Return to top]

Dams Sector

23. *July 1, WANE 15 Fort Wayne* – (Indiana) **Evacuations underway after dams in Wabash, Huntington Counties open.** The U.S. Army Corps of Engineers released water from dams at the Salamoine Reservoir and Roush Lake in Wabash and Huntington Counties June 30 due to the water reaching capacity after a record month of rain. As a precaution people nearby were asked to voluntarily evacuate.
Source: http://wishtv.com/2015/07/01/evacuations-underway-after-dams-in-wabash-huntington-counties-open/

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.